

## COB Review by William Perry

Title: “The Black Book on Corporate Security”

Author: Edited by Larston Publishers (18 Authors)

Length: 439 pages

Price: \$35.00 on-line

Reading time: 40 hours

Reading rating: 3 (1 = very difficult; 10 = very easy)

Overall rating: 3.50 (1 = Average; 4 = outstanding)

Information security is a necessity for an organization that depends upon computers to process critical data for decision making. Securing information assets is even a requirement if the organization is a covered entity under HIPAA, Graham-Leach-Bliley Act and Sarbanes-Oxley Act and other relevant laws and rules. A business owner or executive likely has fiduciary responsibilities to provide for information security. Assuring information assets is now a business process. Indeed, information security should be considered a matter of corporate governance.

The threat environment in which a modern organization now functions is intense. Millions of dollars of proprietary and confidential information are lost each year by unprepared organizations through theft and damage by insiders, hackers, organized crime and corporate espionage. A responsible business owner must assess vulnerabilities, threats and confront the issue of business continuity and resiliency.

One report suggests that 180,000 businesses in existence prior to the terrorist attacks on 9-11-01 just simply disappeared and failed to re-open. Consider how resilient your office and business would be if you had been located in New Orleans during the aftermath of Hurricane Katrina. Would your disaster recovery plan and the robustness of your information security plan make it possible for you to stay in business?

“The Black Book on Corporate Security” is written by eighteen individual experts in the area of information security. Each of the authors specializes in an area of information security. The book, in its entirety, orients corporate leaders into protecting assets in a systematic manner while still being able to flourish and conduct normal business operations.

Readers are exposed to concepts ranging from the broad topic of “information security” to more specific ideas such as how to protect intellectual property and what should be contained in a business continuity plan in the event of a disaster.

The book outlines the latest methods on how to protect corporate assets as well as orients the business leader into how he or she can collaborate with others to enhance organizational security. The authors explain how to conduct a risk analysis and how to determine the return on investment of a security program.

Industry's security best practices are presented in the book and even a discussion on the type of policies that should be in-place is included. A number of very useful security resources are also included in the book's Resource Appendix.

Readers are treated to a relevant digest on information assurance and how to draw-up and implement a corporate security plan in the publication. Any modern day business leader could immediately begin to take appropriate action to enhance information security upon completing the reading of the book. The publication is loaded with practical information.

The subject matter, however, is tightly focused and specialized. Any gaps that you may have in your perceptions on how to protect corporate and information assets will be filled.

William Perry is a Professor of Business Computer Information Systems Department in the College of Business at Western Carolina University. His main research interests include information systems security. For previously reviewed books visit our web site at [www.wcu.edu/cob/](http://www.wcu.edu/cob/).